

ON WELL-ROUNDED SUBLATTICES OF THE HEXAGONAL LATTICE

LENNY FUKSHANSKY, DANIEL MOORE, R. ANDREW OHANA,
AND WHITNEY ZELDOW

ABSTRACT. We produce an explicit parameterization of well-rounded sublattices of the hexagonal lattice in the plane, splitting them into similarity classes. We use this parameterization to study the number, the greatest minimal norm, and the highest signal-to-noise ratio of well-rounded sublattices of the hexagonal lattice of a fixed index. This investigation parallels earlier work by Bernstein, Sloane, and Wright where similar questions were addressed on the space of *all* sublattices of the hexagonal lattice. Our restriction is motivated by the importance of well-rounded lattices for discrete optimization problems. Finally, we also discuss the existence of a natural combinatorial structure on the set of similarity classes of well-rounded sublattices of the hexagonal lattice, induced by the action of a certain matrix monoid.

CONTENTS

1. Introduction	1
2. A Diophantine equation	4
3. The angle form	6
4. The norm form	8
5. Number, minima, and interference of WR sublattices of Λ_h	15
6. Combinatorial structure in the Eisenstein triples	19
References	21

1. INTRODUCTION

Throughout this paper, we will write Λ_h for the hexagonal lattice in \mathbb{R}^2 :

$$(1.1) \quad \Lambda_h := \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix} \mathbb{Z}^2,$$

which is routinely identified with the ring of Eisenstein integers $\mathbb{Z}[\omega]$, where $\omega = e^{\frac{2\pi i}{3}}$. This lattice has many important properties, in particular it solves a variety of classical discrete optimization problems in the plane, such as circle packing and covering problems, kissing number problem, and quantizer problem (see [5] for a detailed account). Not surprisingly, the properties and structure of Λ_h have been

2000 *Mathematics Subject Classification.* Primary: 11H31, 52C15; Secondary: 05B40, 11E45.

Key words and phrases. hexagonal lattice, well-rounded lattices, binary and ternary quadratic forms, Epstein zeta function.

The authors were supported by NSF grant DMS-0755540.

extensively studied for their own sake, as well as for the benefit of many applications arising in engineering and digital communications problems. In particular, a detailed analysis of distribution and optimization properties of sublattices of Λ_h has been carried out by Bernstein, Sloane, and Wright in [3]. It is the goal of this note to continue this investigation, concentrating on the more special class of *well-rounded* (from now on abbreviated as WR) sublattices of Λ_h .

Given a lattice $\Gamma = A\mathbb{Z}^2 \subset \mathbb{R}^2$, where A is a basis matrix, we define its *determinant* to be $\det(\Gamma) = |\det(A)|$, which does not depend on the choice of a basis, and its *minimum* (or *minimal norm*) to be

$$|\Gamma| = \min\{\|\mathbf{y}\|^2 : \mathbf{y} \in \Gamma \setminus \{\mathbf{0}\}\},$$

where $\|\cdot\|$ stands for the usual Euclidean norm. Then each $\mathbf{x} \in \Gamma$ such that $\|\mathbf{x}\|^2 = |\Gamma|$ is called a *minimal vector*, and the set of minimal vectors of Γ is denoted by $S(\Gamma)$. A lattice $\Gamma \subset \mathbb{R}^2$ is called WR if there exists $\mathbf{x}, \mathbf{y} \in S(\Gamma)$ which form a basis for Γ , in which case we call \mathbf{x}, \mathbf{y} a *minimal basis*. This minimal basis is not unique, but it is always possible to select a minimal basis \mathbf{x}, \mathbf{y} for a WR lattice Γ so that the angle θ between these two vectors lies in the interval $[\pi/3, \pi/2]$, and any value of the angle in this interval is possible. From now on when we talk about a minimal basis for a WR lattice in the plane, we will always mean such a choice. Then the angle between minimal basis vectors is an invariant of the lattice, and we call it the *angle of the lattice* Γ , denoted $\theta(\Gamma)$; in other words, if \mathbf{x}, \mathbf{y} is any minimal basis for Γ and γ is the angle between \mathbf{x} and \mathbf{y} , then $\gamma = \theta(\Gamma)$ (see [6] for details and proofs of the basic properties of WR lattices in \mathbb{R}^2). WR lattices are important in coding theory [1] and discrete optimization problems [10]; they also come up in the context of some number theoretic problems, such as Minkowski's conjecture [11] and the linear Diophantine problem of Frobenius [9]. The distribution of WR sublattices of \mathbb{Z}^2 has been studied in [8] and [7].

In [3], the authors consider sublattices of Λ_h of fixed index $J \geq 2$, counting their number (up to *similarity* - to be defined below), and asking which of them have the largest minimum and *signal-to-noise ratio*, abbreviated SNR (to be defined in (1.9) below). They provide only a partial answer for these last two questions, proving that both of these quantities are maximized by an *ideal sublattice* (i.e., a sublattice coming from an ideal in the ring of Eisenstein integers) whenever there exists one of index J . However ideal sublattices, which are a special case of WR sublattices of Λ_h , do not exist for all possible values of the index, and the authors in [3] remark that “for other values of the index there does not seem to be any general rule to identify which sublattices are best.” This motivates a closer investigation of WR sublattices of Λ_h , which, as we show, exist for more values of the index than ideal sublattices. In this paper we discuss WR sublattices of Λ_h , giving an explicit description and parameterization for all of them. We then use this parameterization to study their properties with a view toward the discrete optimization questions analogous to those asked in [3].

In order to state our results the notion of similarity of lattices is needed. Two lattices $\Gamma_1, \Gamma_2 \subset \mathbb{R}^2$ are called *similar*, denoted $\Gamma_1 \sim \Gamma_2$, if there exists a nonzero real number α and a 2×2 real orthogonal matrix A such that $\Gamma_2 = \alpha A \Gamma_1$. Similarity is easily seen to be an equivalence relation, and we refer to the equivalence classes under this relation as similarity classes of lattices. WR lattices can only be similar to WR lattices, hence it makes sense to talk about similarity classes of WR lattices. In fact, it is easy to notice that two WR lattices $\Gamma_1, \Gamma_2 \subset \mathbb{R}^2$ are similar if and only

if $\theta(\Gamma_1) = \theta(\Gamma_2)$ (see [6] for a proof). Therefore the set of all similarity classes of WR lattices is bijectively parameterized by the set of all possible values of the angle, which is the interval $[\pi/3, \pi/2]$. On the other hand, this parameterization becomes much less trivial if we talk about similarity classes of WR sublattices of Λ_h . Let us write $\text{WR}(\Lambda_h)$ for the set of all WR sublattices of Λ_h , and for each $\Gamma \in \text{WR}(\Lambda_h)$ define

$$(1.2) \quad \langle \Gamma \rangle := \{ \Omega \in \text{WR}(\Lambda_h) : \Omega \sim \Gamma \} = \{ \Omega \in \text{WR}(\Lambda_h) : \theta(\Omega) = \theta(\Gamma) \},$$

and let

$$\text{Sim}_{\text{WR}}(\Lambda_h) := \{ \langle \Gamma \rangle : \Gamma \in \text{WR}(\Lambda_h) \}.$$

Then it is clear that $\text{Sim}_{\text{WR}}(\Lambda_h)$ is bijectively parameterized by some subset of the interval $[\pi/3, \pi/2]$, and the natural question is what is this subset? Our main result answers this question in detail.

Theorem 1.1. *Let*

$$(1.3) \quad C_h = \{ \theta \in [\pi/3, \pi/2] : \theta = \theta(\Gamma) \text{ for some } \Gamma \in \text{WR}(\Lambda_h) \}.$$

Then $\theta \in C_h$ if and only if

$$(1.4) \quad \cos \theta = \frac{1}{2} \times \frac{|n^2 + 2mn - 2m^2|}{n^2 - mn + m^2}$$

for some $m, n \in \mathbb{Z}$ such that $\gcd(m, n) = 1$, $1 \leq \frac{m}{n} \leq 2$, and $3 \nmid (m + n)$. For each $\theta \in C_h$, let us write $C_h(\theta)$ for the corresponding similarity class. Then $C_h(\theta) = \langle \Gamma_\theta \rangle$, where

$$(1.5) \quad \Gamma_\theta = \frac{1}{2} \begin{bmatrix} m+n & m-2n \\ (m-n)\sqrt{3} & m\sqrt{3} \end{bmatrix} \mathbb{Z}^2 \subseteq \Lambda_h,$$

for the integers m, n corresponding to θ as above, and for each $\Gamma \in C_h(\theta)$,

$$(1.6) \quad |\Gamma| \geq |\Gamma_\theta| = n^2 - mn + m^2, \quad |\Lambda_h : \Gamma| = \frac{\det(\Gamma)}{\det(\Lambda_h)} \geq |\Lambda_h : \Gamma_\theta| = (2m - n)n.$$

In fact,

$$(1.7) \quad C_h(\theta) = \left\{ \sqrt{k} A \Gamma_\theta \subseteq \Lambda_h : k \in \mathbb{Z}_{>0}, A \in O_2(\mathbb{R}) \right\},$$

where all the possible values of k and the corresponding matrices A are explicitly described in Lemma 4.8 below, and all possible values of $|\Lambda_h : \Gamma|$ for $\Gamma \in \text{WR}(\Lambda_h)$ are described in Corollary 4.9 below. Due to the properties (1.6) and (1.7), we call Γ_θ a minimal sublattice in its similarity class.

Remark 1.1. Notice in particular that $\pi/3 \in C_h$ with the corresponding pair $(m, n) = (1, 1)$, and $C_h(\pi/3) = \langle \Lambda_h \rangle$. As is indicated in [3], ideal sublattices of Λ_h are precisely those that are similar to Λ_h , hence the ideal sublattices form only one similarity class $C_h(\pi/3)$ in the infinite set $\text{Sim}_{\text{WR}}(\Lambda_h)$ of similarity classes of WR sublattices of Λ_h , parameterized by C_h . On the other hand, $\pi/2 \notin C_h$, since

$$n^2 + 2mn - 2m^2 = (m + n)^2 - 3m^2 \neq 0,$$

as $3 \nmid (m + n)$. This is the complete opposite of the situation for WR sublattices of \mathbb{Z}^2 (identified with the ring of Gaussian integers), as studied in [8]: the similarity class of ideal sublattices of \mathbb{Z}^2 corresponds to the value of the angle $\pi/2$, while there is no similarity class of WR sublattices of \mathbb{Z}^2 corresponding to $\pi/3$.

We prove Theorem 1.1 in section 4. Our proof is based on a parameterization of lattices in question in terms of integral solution to a certain Diophantine equation, given by a ternary quadratic form. We produce such a parameterization of solutions for a family of integral ternary quadratic form equations in section 2 with the use of a simple geometric argument. In section 3 we show how a particular such quadratic form can be used to parameterize similarity classes of WR lattices by means of looking at the corresponding values of the angle. However the parameterization of section 3 does not necessarily produce a minimal lattice for each similarity class. The main goal of section 4 then is to go one step further and produce a description of similarity classes in terms of minimal lattices.

In section 5 we discuss the three optimization questions for WR sublattices of Λ_h , that are analogous to the questions considered in [3]. These questions are concerned with counting the number, as well as maximizing the minimal norm and signal-to-noise ratio of WR sublattices of Λ_h of a fixed index. Given a sublattice $\Gamma \in \text{WR}(\Lambda_h)$, we can regard its nonzero points as transmitters which interfere with the transmitter at the origin, and then a standard measure of the *total interference* of Γ is given by $E_\Gamma(2)$, where

$$(1.8) \quad E_\Gamma(s) = \sum_{\mathbf{x} \in \Gamma \setminus \{\mathbf{0}\}} \frac{1}{\|\mathbf{x}\|^{2s}}$$

is the Epstein zeta-function of Γ , and the signal-to-noise ratio of Γ is defined by

$$(1.9) \quad \text{SNR}(\Gamma) = 10 \log_{10} \frac{1}{9E_\Gamma(2)},$$

as in [3]. To maximize $\text{SNR}(\Gamma)$ on the set of all WR sublattices of Λ_h of a fixed index J is the same as to minimize $E_\Gamma(2)$. In particular, we show (Lemma 5.2 below) that $\text{SNR}(\Gamma)$ is maximized by the same sublattice of fixed index J that maximizes $|\Gamma|$, and vice versa. This is not always so for non-WR sublattices of Λ_h , as demonstrated in [3].

Finally, in section 6 we discuss a combinatorial structure on the set of all similarity classes of WR sublattices of Λ_h , induced by the action of a certain submonoid of $\text{GL}_3(\mathbb{Z})$.

2. A DIOPHANTINE EQUATION

In this section we use a simple geometric idea to construct an explicit parameterization of integral zeros of a certain integral ternary quadratic form. We later use this parameterization to prove Theorem 1.1.

Lemma 2.1. *Consider the Diophantine equation*

$$(2.1) \quad \alpha x^2 + \beta xy + \gamma y^2 = \delta z^2,$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ with $\beta^2 \neq 4\alpha\gamma$ and $\delta \neq 0$. Then either this equation has no integral solutions with $z \neq 0$, or all such solutions (x, y, z) of (2.1) are rational multiples of

$$(2.2) \quad \begin{aligned} x &= \gamma n(an - 2bm) - (\alpha a + \beta b)m^2, \\ y &= \alpha m(bm - 2an) - (\gamma b + \beta a)n^2, \\ z &= \pm c(\alpha m^2 + \beta mn + \gamma n^2), \end{aligned}$$

where $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$ and $m \geq 0$; here (a, b, c) is any integral solution to (2.1) with $c \neq 0$. In this later case, every multiple of (2.2) is a solution to (2.1) by homogeneity of the equation (2.1).

Proof. Suppose there exists an integer solution (a, b, c) to (2.1) with $c \neq 0$, and consider the rational curve

$$(2.3) \quad \frac{\alpha}{\delta} u^2 + \frac{\beta}{\delta} uv + \frac{\gamma}{\delta} v^2 = 1,$$

where $u = x/z$, $v = y/z$. The point $(a/c, b/c)$ lies on this curve, and let (u, v) be any other rational point on the curve. If $v = b/c$, then we must have $\alpha \neq 0$ and $u = -a/c - b\beta/c\alpha$, and so the point (u, v) corresponds to the solution $(-a\alpha - b\beta, b\alpha, c\alpha)$ of (2.1), obtained from (2.2) when $m = 1$, $n = 0$. Otherwise, there exists a unique line with rational slope through the points $(a/c, b/c)$ and (u, v) . Therefore there exists $m/n \in \mathbb{Q}$ such that

$$(2.4) \quad u = \frac{m}{n} \left(v - \frac{b}{c} \right) + \frac{a}{c}.$$

Substituting (2.4) into (2.3) and solving for v , we obtain:

$$(2.5) \quad v = \frac{\alpha m(bm - 2an) - (\gamma b + \beta a)n^2}{c(\alpha m^2 + \beta mn + \gamma n^2)}.$$

Now substituting (2.5) into (2.4), we have:

$$(2.6) \quad u = \frac{\gamma n(an - 2bm) - (\alpha a + \beta b)m^2}{c(\alpha m^2 + \beta mn + \gamma n^2)}.$$

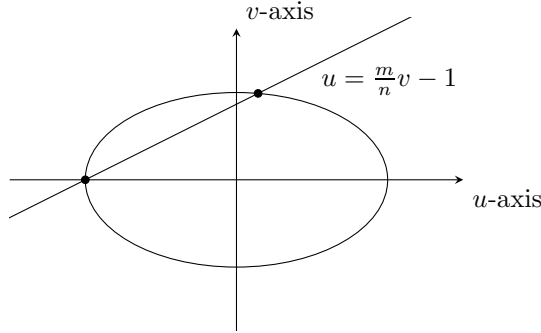


FIGURE 1. Algorithm for $x^2 + 3y^2 = z^2$ with the solution $(-1, 0, 1)$.

As m, n range over all coprime pairs of integers, (2.6) and (2.5) give coordinates of all rational points (u, v) on the curve (2.3), and therefore every integral solution (x, y, z) of (2.1) is a rational multiple of (2.2) for some m, n . \square

Remark 2.1. Notice that for every two different relatively prime pairs of integers m_1, n_1 and m_2, n_2 , the corresponding solutions (x_1, y_1, z_1) and (x_2, y_2, z_2) of (2.1) as in (2.2) represent different projective points, i.e., there does not exist a real number t such that $(x_1, y_1, z_1) = t(x_2, y_2, z_2)$. Hence (2.2) describes all the distinct rational projective points on the hypersurface given by the equation (2.1). We will be especially interested in *primitive* integral solutions to equations of the form (2.1),

i.e., representatives $(x, y, z) \in \mathbb{Z}^3$ of their projective points described by (2.2) with $\gcd(x, y, z) = 1$.

3. THE ANGLE FORM

In this section we construct our first parameterization of WR sublattices of Λ_h .

Lemma 3.1. *For every $\Gamma \in \text{WR}(\Lambda_h)$,*

$$(3.1) \quad \cos \theta(\Gamma) = \frac{p}{q} \leq \frac{1}{2}, \quad \sin \theta(\Gamma) = \frac{r}{q} \sqrt{3} \geq \frac{\sqrt{3}}{2},$$

where the triple $(p, r, q) \in \mathbb{Z}_{\geq 0}^3$ is relatively prime.

Proof. Let Γ be a WR sublattice of Λ_h . Then there exist $a, b, c, d \in \mathbb{Z}$ such that

$$\Gamma = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix} \mathbb{Z}^2 = \begin{bmatrix} a - b/2 & c - d/2 \\ b\sqrt{3}/2 & d\sqrt{3}/2 \end{bmatrix} \mathbb{Z}^2,$$

where

$$\mathbf{x} := \begin{bmatrix} a - b/2 \\ b\sqrt{3}/2 \end{bmatrix}, \quad \mathbf{y} := \begin{bmatrix} c - d/2 \\ d\sqrt{3}/2 \end{bmatrix}$$

is a minimal basis for Γ . Hence

$$\|\mathbf{x}\|^2 = a^2 - ab + b^2 = c^2 - cd + d^2 = \|\mathbf{y}\|^2,$$

and

$$\frac{1}{2} \geq \cos \theta(\Gamma) = \frac{\mathbf{x}^t \mathbf{y}}{\|\mathbf{x}\| \|\mathbf{y}\|} = \frac{a(2c - d) + b(2d - c)}{2(a^2 - ab + b^2)} \in \mathbb{Q}.$$

Then

$$\begin{aligned} \sin \theta(\Gamma) &= \sqrt{1 - \cos^2 \theta(\Gamma)} = \sqrt{1 - \frac{(2ac + 2bd - ad - bc)^2}{4(a^2 - ab + b^2)^2}} \\ &= \frac{ad - bc}{2(a^2 - ab + b^2)} \sqrt{3} \geq \frac{\sqrt{3}}{2}. \end{aligned}$$

Therefore (3.1) is satisfied with

$$(3.2) \quad p = a(2c - d) + b(2d - c), \quad r = ad - bc, \quad q = 2(a^2 - ab + b^2),$$

which completes the proof of the lemma. \square

Notice, on the other hand, that if the triple (p, r, q) is as in (3.1) for some $\Gamma \in \text{WR}(\Lambda_h)$, then

$$(3.3) \quad p^2 + 3r^2 = q^2,$$

which is a particular instance of the equation (2.1) with $\alpha = \delta = 1$, $\beta = 0$, and $\gamma = 3$. We will refer to the binary integral quadratic form $p^2 + 3r^2$ on the left hand side of (3.3) as the *angle form* because of the above connection of the integral solutions of (3.3) to values of trigonometric functions of the angles of lattices from $\text{WR}(\Lambda_h)$. In fact, Lemma 2.1 (see also Figure 1 above) guarantees that all projectively distinct integer solutions $(p, r, q) \in \mathbb{Z}_{>0}^3$ of (3.3) are given by

$$(3.4) \quad p = m^2 - 3n^2, \quad r = 2mn, \quad q = m^2 + 3n^2,$$

where m and n are coprime integers. If we only consider triples (p, r, q) as in (3.4) with $\sqrt{3} < m/n \leq 3$, then there exists an angle $\theta \in [\pi/3, \pi/2)$ such that

$$(3.5) \quad \cos \theta = \frac{p}{q}, \quad \sin \theta = \frac{r}{q}\sqrt{3},$$

and vice versa. Then $\theta \in C_h$ defines the similarity class $C_h(\theta)$ of WR sublattices of Λ_h , as described in the statement of Theorem 1.1. We will now construct a sublattice Ω_θ of Λ_h in $C_h(\theta)$ using our parameterization.

Lemma 3.2. *Let m and n be coprime positive integers with $\sqrt{3} < \frac{m}{n} \leq 3$, and let (p, r, q) be as in (3.4). Let θ be as in (3.5). Then the lattice*

$$(3.6) \quad \Omega_\theta := \begin{bmatrix} m & m \\ n\sqrt{3} & -n\sqrt{3} \end{bmatrix} \mathbb{Z}^2$$

is in $WR(\Lambda_h)$, and has the following properties:

$$|\Omega_\theta| = q, \quad \det(\Omega_\theta) = r\sqrt{3}, \quad |\Lambda_h : \Omega_\theta| = 2r, \quad \text{and} \quad \Omega_\theta \in C_h(\theta).$$

Hence $C_h(\theta) = \langle \Omega_\theta \rangle$.

Proof. First notice that Ω_θ , as defined in (3.6), is given by

$$\Omega_\theta = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix} \begin{bmatrix} m+n & m-n \\ 2n & -2n \end{bmatrix} \mathbb{Z}^2,$$

hence it is a sublattice of Λ_h . Also

$$\det(\Omega_\theta) = 2mn\sqrt{3} = r\sqrt{3},$$

and

$$|\Lambda_h : \Omega_\theta| = \frac{\det \Gamma}{\det \Lambda_h} = 4mn = 2r.$$

Now let

$$\mathbf{x} = \begin{bmatrix} m \\ n\sqrt{3} \end{bmatrix}, \quad \mathbf{y} = \begin{bmatrix} m \\ -n\sqrt{3} \end{bmatrix},$$

and notice that $\|\mathbf{x}\| = \|\mathbf{y}\| = \sqrt{m^2 + 3n^2} = \sqrt{q}$. Moreover, if ν is the angle between these two vectors, then

$$\cos \nu = \frac{\mathbf{x}^t \mathbf{y}}{\|\mathbf{x}\| \|\mathbf{y}\|} = \frac{m^2 - 3n^2}{q} = \frac{p}{q},$$

hence this angle is precisely θ . The condition $\sqrt{3} < \frac{m}{n} \leq 3$ implies that $\pi/3 \leq \theta < \pi/2$, meaning that for any $s, t \in \mathbb{Z}$

$$\|s\mathbf{x} + t\mathbf{y}\|^2 = s^2\|\mathbf{x}\|^2 + 2st\|\mathbf{x}\|\|\mathbf{y}\|\cos \theta + t^2\|\mathbf{y}\|^2 \geq \|\mathbf{x}\|^2 = \|\mathbf{y}\|^2,$$

hence \mathbf{x}, \mathbf{y} form a minimal basis for Ω_θ . Therefore $|\Omega_\theta| = q$, and $\Omega_\theta \in C_h(\theta)$. \square

Thus similarity classes of WR sublattices of Λ_h are in bijective correspondence with triples (p, r, q) as defined in (3.4) satisfying $\sqrt{3} < m/n \leq 3$ and $\gcd(m, n) = 1$. In other words, we obtained a parameterization of the set C_h by a subset of projectively distinct zeros of the angle form. The construction of Lemma 3.2 however does not always produce *minimal* WR sublattices of Λ_h in the sense of (1.6) of Theorem 1.1. For instance, $\Lambda_h \in C_h(\pi/3)$, while

$$\Omega_{\pi/3} = \begin{bmatrix} 3 & 3 \\ \sqrt{3} & -\sqrt{3} \end{bmatrix} \mathbb{Z}^2$$

with $|\Omega_{\pi/3}| = 12$ (recall that $|\Lambda_h| = 1$). Our next goal is to provide a parameterization of $\text{Sim}_{\text{WR}}(\Lambda_h)$ by minimal sublattices, which we do in the next section.

4. THE NORM FORM

The main goal of this section is to prove Theorem 1.1. We start by considering another particular instance of the equation (2.1) with $\alpha = \gamma = \delta = 1$ and $\beta = -1$, which we write as

$$(4.1) \quad a^2 - ab + b^2 = c^2,$$

where the left hand side of (4.1) is the *norm form* of the hexagonal lattice with respect to the basis matrix $\begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}$, which is precisely the norm in the ring of Eisenstein integers $\mathbb{Z}[\omega]$. We will call every solution $(a, b, c) \in \mathbb{Z}_{\geq 0}^3 \setminus \{(0, 0, 0)\}$ to (4.1) an *Eisenstein triple*, and we call an Eisenstein triple (a, b, c) *primitive* if $a \leq b$ and $\gcd(a, b, c) = 1$. Then we have the following simple corollary of Lemma 2.1.

Corollary 4.1. *All Eisenstein triples are positive rational multiples of*

$$(4.2) \quad a = m(2n - m), \quad b = n(2m - n), \quad c = m^2 - mn + n^2,$$

where $m, n \in \mathbb{Z}_{>0}$ with $\gcd(m, n) = 1$ and $\frac{1}{2} \leq \frac{m}{n} \leq 2$. Moreover, every integer triple (a, b, c) that is a positive rational multiple of (4.2) for some m, n satisfying the above conditions is an Eisenstein triple by homogeneity of the equation (4.1).

Proof. We apply Lemma 2.1 to the equation (4.1) with the particular solution $(-1, -1, 1)$ as in Figure 2 below. To obtain the restrictions on m and n , first notice

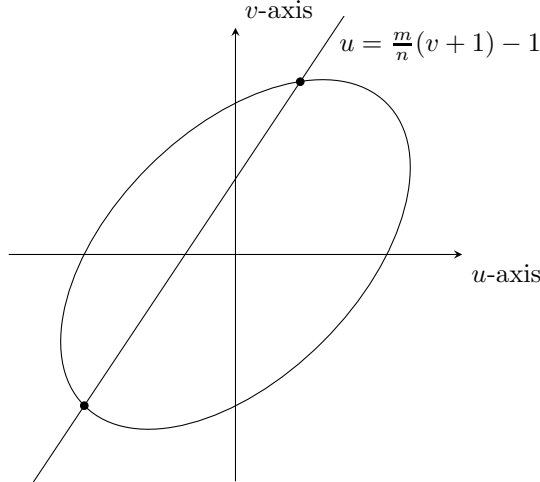


FIGURE 2. Algorithm for $x^2 - xy + y^2 = z^2$ with the solution $(-1, 1, 1)$.

that since $(a, b, c) \in \mathbb{Z}_{\geq 0}^3$ and $m \geq 0$ we have $0 \leq 2n - m$, hence $n \geq \frac{m}{2} \geq 0$ and $\frac{m}{n} \leq 2$ ($n > 0$ since $n = 0$ would imply $m = n = 0 \Rightarrow a = b = c = 0$). Since $b \geq 0$, we must have $0 \leq 2m - n$. Since $n > 0$, we have $m > 0$, and hence $\frac{1}{2} \leq \frac{m}{n}$. \square

Here is a brief outline of our strategy for the remainder of this section. We will first use Corollary 4.1 to give a parameterization of the primitive Eisenstein triples. We will then relate primitive Eisenstein triples to solutions of the angle form equation, thus obtaining a new parameterization for the similarity classes of WR sublattices of Λ_h . This new parameterization will then be used to produce minimal lattices for the similarity classes.

Since we are trying to produce primitive Eisenstein triples, we may assume that integers m, n in (4.2) are relatively prime. We start by proving that in this case $\gcd(a, b, c) = 1$ or 3.

Lemma 4.2. *Let (a, b, c) be a triple of the form (4.2) with relatively prime $m, n \in \mathbb{Z}$, then $\gcd(a, b, c) = 1$ or 3. More precisely:*

- (1) $\gcd(a, b, c) = 3$ if and only if $3 \mid (m + n)$.
- (2) $\gcd(a, b, c) = 1$ if and only if $3 \nmid (m + n)$.

Proof. Suppose first that $m + n = 3k$ for some integer k , then

$$a = 3m(2k - m), \quad b = 3n(2k - n), \quad c = 3(km - mn + kn),$$

so $3 \mid \gcd(a, b, c)$. Now suppose that there is some prime p dividing $\frac{\gcd(a, b, c)}{3}$, then $p \mid m(2k - m), n(2k - n)$. Since $\gcd(m, n) = 1$, it must be that either $p \mid m, 2k - n$ or $p \mid 2k - m, n$. Notice that $n = 3k - m$ and $2k - n = m - k$. First suppose that $p \mid m, 2k - n$, then

$$p \mid m - (m - k) = k \implies p \mid 2k - (2k - n) = n,$$

which is a contradiction. Next suppose that $p \mid 2k - m, n$, then

$$p \mid (3k - m) - (2k - m) = k \implies p \mid 2k - (2k - m) = m,$$

which is a contradiction. Therefore $\gcd(a, b, c) = 3$.

Conversely, if $\gcd(a, b, c) = 3$, then

$$3 \mid a + b = -((m + n)^2 - 6mn),$$

hence $3 \mid m + n$.

Next assume that $3 \nmid (m + n)$. Suppose that $\gcd(a, b, c) > 1$, then there exists a prime p such that $p \mid a, b$. Suppose that $p \mid (m - n)$, then

$$p \mid (b + (m - n)^2) = m^2, \quad p \mid (a + (m - n)^2) = n^2,$$

which contradicts co-primality of m, n . Therefore $p \nmid (m - n)$. Moreover, $p \nmid m, n$: if, for instance, $p \mid m$, then $p \mid (2nm - b) = n^2$, which is a contradiction; similarly, if $p \mid n$, then p must divide m . Now notice that

$$p \mid (b - a) = (m - n)(m + n),$$

and since $p \nmid (m - n)$, p must divide $m + n$. Therefore

$$p \mid (b + (m + n)^2) = m(m + 4n), \quad p \mid (a + (m + n)^2) = n(n + 4m).$$

Since $p \nmid m, n$, we find that $p \mid (m + 4n), (n + 4m)$, and hence

$$p \mid ((n + 4m) - (m + 4n)) = 3(m - n).$$

Since $p \nmid (m - n)$, it must be the case that $p = 3$, contradicting our assumption that $3 \nmid (m + n)$. Thus $\gcd(a, b, c) = 1$.

Conversely, suppose $\gcd(a, b, c) = 1$. Suppose $3 \mid (m + n)$. Then

$$3 \mid (m - n)(m + n) = b - a, \quad 3 \mid -((m + n)^2 - 6mn) = a + b,$$

and so

$$3 \mid (b - a) + (b + a) = 2b, \quad 3 \mid (b - a) - (b + a) = -2a.$$

Hence $3 \mid a, b$, which is a contradiction, so $3 \nmid (m + n)$. This completes the proof of the lemma. \square

Remark 4.1. A parameterization of primitive Eisenstein triples partially similar to our Corollary 4.1 and Lemma 4.2 (but using different arguments) has been obtained in [2]. We include our results here since the details of this parameterization are important to our description of similarity classes of WR sublattices of Λ_h .

We can now give a parameterization of primitive Eisenstein triples. Notice that for each primitive Eisenstein triple (a, b, c) , $(b - a, b, c)$ is also a primitive Eisenstein triple, and $(b - (b - a), b, c) = (a, b, c)$, i.e., the map taking (a, b, c) to $(b - a, b, c)$ is an involution on the set of primitive Eisenstein triples. We will call two triples like this *associated*, and write $\langle a, b, c \rangle$ for the associated pair. Then the set of all primitive Eisenstein triples can be split into a collection of associated pairs.

Lemma 4.3. *A pair of vectors $(a, b, c), (b - a, b, c) \in \mathbb{Z}_{\geq 0}^3$ is an associated pair of primitive Eisenstein triples if and only if precisely one of these triples is given by (4.2) for some integers m, n satisfying*

- (1) $m, n > 0$ and $\gcd(m, n) = 1$
- (2) $1 \leq \frac{m}{n} \leq 2$
- (3) $3 \nmid (m + n)$.

Proof. Suppose first that (a, b, c) is as in (4.2) with m, n satisfying the above-stated conditions (1), (2), (3). Then (a, b, c) is an Eisenstein triple by Corollary 4.1, and $\gcd(a, b, c) = 1$ by Lemma 4.2. Moreover,

$$a = 2mn - m^2 \leq 2mn - n^2 = b,$$

and hence (a, b, c) is a primitive Eisenstein triple.

Now assume that (a, b, c) is a primitive Eisenstein triple, then so is $(b - a, b, c)$. Corollary 4.1 implies that

$$(a, b, c) = \frac{1}{g}(a', b', c'),$$

where (a', b', c') is an Eisenstein triple given by (4.2) with m, n satisfying condition (1) and $\frac{1}{2} \leq \frac{m}{n} \leq 2$, and $g = \gcd(a', b', c')$. First suppose that $\frac{m}{n} < 1$. This means that

$$(4.3) \quad a = 2mn - m^2 > 2mn - n^2 = b,$$

which contradicts (a, b, c) being primitive. Therefore the integers m, n must also satisfy condition (2). Now Lemma 4.2 implies that m, n satisfy condition (3) if and only if $g = 1$, and $g = 3$ otherwise. Suppose $g = 3$. Then it can be easily verified that $(a_1, b_1, c_1) := (b - a, b, c)$ is given by (4.2) with positive integers

$$m_1 = \frac{m + n}{3}, \quad n_1 = \frac{2m - n}{3}.$$

Suppose that an integer $t \mid m_1, n_1$. Then

$$t \mid m_1 + n_1 = m, \quad 2m_1 - 2n_1 = n,$$

but $\gcd(m, n) = 1 \Rightarrow \gcd(m_1, n_1) = 1$, hence m_1, n_1 satisfy condition (1). By the same argument as in (4.3) with a_1, b_1, m_1, n_1 instead of a, b, m, n we conclude

that m_1, n_1 satisfy condition (2). Finally, suppose that $3 \mid (m_1 + n_1) = m$. Since $3 \mid (m + n)$, we conclude that $3 \mid n$, meaning that m, n are not relatively prime, which is a contradiction. Therefore m_1, n_1 satisfy condition (3) as well.

Now suppose that $g = 1$, then it is easy to verify that

$$(b - a, b, c) = \frac{1}{3}(a_2, b_2, c_2),$$

where (a_2, b_2, c_2) is given by (4.2) with positive integers

$$m_2 = m + n, \quad n_2 = 2m - n.$$

By the argument in the proof of Lemma 2.1 (see also Remark 2.1), there cannot exist another pair m'_2, n'_2 parameterizing the triple $(b - a, b, c)$. Hence we showed that *precisely* one of the triples in an associated pair is given by (4.2) with integers m, n satisfying (1)-(3). This completes the proof of the lemma. \square

Our next step is to relate primitive Eisenstein triples to solutions of the angle form equation (3.3). For each vector $(x, y, z) \in \mathbb{R}^3$, we will write $[x, y, z]$ to denote the corresponding projective point. First define

$$\begin{aligned} \mathfrak{A} &= \{[p, r, q] : (p, r, q) \text{ satisfying (3.4), } \sqrt{3} < m/n \leq 3\} \\ (4.4) \quad &= \{[p, r, q] : (p, r, q) \text{ satisfying (3.3), } 0 < p/q \leq 1/2\}. \end{aligned}$$

Next, for each associated pair $\langle a, b, c \rangle$ of primitive Eisenstein triples, let us write $\{a, b, c\}$ for the associated pair of the corresponding projective points, $[a, b, c]$ and $[b - a, b, c]$, and define \mathfrak{E} to be the set of all such associated pairs. Let $T : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ be a bijective linear map, given by the matrix

$$\begin{bmatrix} -2 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

Notice that for each $\{a, b, c\} \in \mathfrak{E}$ with $\gcd(a, b, c) = 1$

$$T(a, b, c) = (b - 2a, b, 2c), \quad T(b - a, b, c) = (-(b - 2a), b, 2c),$$

and

$$(b - 2a)^2 + 3b^2 = (2c)^2,$$

meaning that precisely one triple from the associated pair $\{a, b, c\}$ maps to the triple $(|b - 2a|, b, 2c)$ under T . Since $a \leq b$ and $\gcd(a, b) = 1$ (meaning in particular that $2a \neq b$),

$$0 < |b - 2a|^2 = 4a(a - b) + b^2 \leq a(a - b) + b^2 = c^2,$$

therefore $0 < |b - 2a|/2c \leq 1/2$, and so $[|b - 2a|, b, 2c] \in \mathfrak{A}$. Now consider the map $T^{-1} : \mathbb{R}^3 \rightarrow \mathbb{R}^3$, given by the inverse matrix of T

$$\begin{bmatrix} -1/2 & 1/2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1/2 \end{bmatrix},$$

and notice that for every $[p, r, q] \in \mathfrak{A}$,

$$T^{-1}(p, r, q) = \left(\frac{r - p}{2}, r, \frac{q}{2} \right)$$

is a solution to (4.1). Moreover, if

$$p = m^2 - 3n^2, \quad r = 2mn, \quad q = m^2 + 3n^2,$$

where m and n are coprime integers with $m = \alpha n$ for some real $\sqrt{3} < \alpha \leq 3$, then

$$r - p = (2\alpha - \alpha^2 + 3)n^2 \geq 0,$$

and $(r-p)/2 \leq r$. Hence $T^{-1}(p, r, q)$ is a representative of a projective point defined by some primitive Eisenstein triple. We have proved the following lemma.

Lemma 4.4. *There is a bijective correspondence between the sets \mathfrak{A} and \mathfrak{E} as described above.*

Now this bijection can be easily used to relate primitive Eisenstein triples to well-rounded sublattices of the hexagonal lattice.

Corollary 4.5. *Let C_h be as in (1.3), and for every $\theta \in C_h$ let $C_h(\theta)$ be the corresponding similarity class of WR sublattices of Λ_h , as in the statement of Theorem 1.1. Then for each $C_h(\theta)$ there exist exactly two primitive Eisenstein triples (a, b, c) and $(b-a, b, c)$ such that*

$$(4.5) \quad \cos \theta = \frac{|b-2a|}{2c} = \frac{|b-2(b-a)|}{2c}.$$

Conversely, for each primitive Eisenstein triple (a, b, c) there exists a unique similarity class $C_h(\theta)$ with $\theta \in C_h$ satisfying (4.5).

Proof. Notice that the quotients in (4.5) only depend on the associated pair of projective points $\{a, b, c\}$, not on actual choice of representatives of these points. The statement of the corollary now follows by combining Lemma 4.4 with the parameterization of section 3. \square

Next we use the parameterization given in Lemma 4.3 to construct a WR sublattice in each similarity class $C_h(\theta)$ with θ as in (4.5).

Lemma 4.6. *Let (a, b, c) be a primitive Eisenstein triple, and let m, n be the integers parameterizing either (a, b, c) or $(b-a, b, c)$, as defined in Lemma 4.3. Let θ be as given by (4.5). Define*

$$(4.6) \quad \Gamma_\theta = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix} \begin{bmatrix} m & m-n \\ m-n & m \end{bmatrix} \mathbb{Z}^2 = \frac{1}{2} \begin{bmatrix} m+n & m-2n \\ (m-n)\sqrt{3} & m\sqrt{3} \end{bmatrix} \mathbb{Z}^2.$$

Then $\Gamma_\theta \in \text{WR}(\Lambda_h)$ is such that $C_h(\theta) = \langle \Gamma_\theta \rangle$. Moreover,

$$|\Gamma_\theta| = c, \quad \det \Gamma_\theta = b \frac{\sqrt{3}}{2}, \quad |\Lambda_h : \Gamma_\theta| = b.$$

Proof. By definition (4.6), Γ_θ is a sublattice of Λ_h . First we see that

$$\det \Gamma_\theta = \det \begin{bmatrix} m & m-n \\ m-n & m \end{bmatrix} \det \Lambda_h = n(2n-m) \frac{\sqrt{3}}{2} = b \frac{\sqrt{3}}{2},$$

and so

$$|\Lambda_h : \Gamma_\theta| = \frac{\det \Gamma_\theta}{\det \Lambda_h} = b.$$

Now let

$$\mathbf{x} = \frac{1}{2} \begin{bmatrix} m+n \\ (m-n)\sqrt{3} \end{bmatrix}, \quad \mathbf{y} = \pm \frac{1}{2} \begin{bmatrix} m-2n \\ m\sqrt{3} \end{bmatrix},$$

where the \pm choice in the definition of \mathbf{y} is such that $\mathbf{x}^t \mathbf{y} > 0$. Notice that $\|\mathbf{x}\|^2 = \|\mathbf{y}\|^2 = m^2 - mn + n^2 = c$. Moreover, the cosine of the angle between these two vectors is equal to

$$\frac{\mathbf{x}^t \mathbf{y}}{\|\mathbf{x}\| \|\mathbf{y}\|} = \pm \frac{2m^2 - 2mn - n^2}{2c} = \frac{|b - 2a|}{2c},$$

hence this angle is precisely θ . By construction, $\pi/3 \leq \theta < \pi/2$, which means that any integral linear combination of the vectors \mathbf{x} and \mathbf{y} has norm at least as large as the norm of these vectors, hence they form a minimal basis for Γ_θ . This implies that $|\Gamma_\theta| = c$ and $\Gamma_\theta \in C_h(\theta)$, which means that $C_h(\theta) = \langle \Gamma_\theta \rangle$. \square

Now we show that the sublattice constructed in Lemma 4.6 is minimal in its similarity class, as defined in the statement Theorem 1.1.

Lemma 4.7. *Let Γ_θ be defined as in (4.6) and let $\Omega \in C_h(\theta)$, then $|\Gamma_\theta| \leq |\Omega|$. Hence Γ_θ is a minimal sublattice in the similarity class $C_h(\theta)$.*

Proof. Since $\Omega \sim \Gamma_\theta$, there exists $0 \neq \alpha \in \mathbb{R}$ and a 2×2 real orthogonal matrix A such that

$$\Omega = \alpha A \Gamma_\theta.$$

Notice that $\alpha^2 c = |\Omega| \in \mathbb{Z}$ and $\alpha^2 b = |\Lambda_h : \Omega| \in \mathbb{Z}$, hence $\alpha^2 \in \mathbb{Q}$; let us write $\alpha^2 = p/q$ with $\gcd(p, q) = 1$. Then $q^2 \mid b$ and $q^2 \mid c$, but $\gcd(b, c) = 1$ and so $\alpha^2 \in \mathbb{Z}_{\geq 0}$. Therefore $|\Gamma_\theta| \leq \alpha^2 |\Gamma_\theta| = |\Omega|$. \square

Therefore for each $\theta \in C_h$,

$$(4.7) \quad C_h(\theta) = \left\{ \sqrt{k} A \Gamma_\theta \subseteq \Lambda_h : k \in \mathbb{Z}_{>0}, A \in O_2(\mathbb{R}) \right\}.$$

What can be said about k and A ? We have the following lemma.

Lemma 4.8. *Let*

$$D = \{1\} \cup \{d = p_1 \dots p_s : p_1, \dots, p_s \text{ distinct primes } \equiv 1 \pmod{3}\},$$

and for each $d \in D$ let

$$S(d) = \{(p, r, q) : p^2 + 3r^2 = dq^2\}$$

as given by the parameterization of Lemma 2.1 with $\alpha = 1, \beta = 0, \gamma = 3, \delta = d$. A lattice $\Gamma \in C_h(\theta)$ if and only if $\Gamma = \sqrt{k} A \Gamma_\theta$ where one of the following two conditions hold:

- (1) $k = j^2 d$ for some $j \in \mathbb{Z}_{>0}$, $d \in D$, and

$$A = \begin{bmatrix} \frac{p}{q\sqrt{d}} & -\frac{r\sqrt{3}}{q\sqrt{d}} \\ \frac{r\sqrt{3}}{q\sqrt{d}} & \frac{p}{q\sqrt{d}} \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} \frac{p}{q\sqrt{d}} & \frac{r\sqrt{3}}{q\sqrt{d}} \\ \frac{r\sqrt{3}}{q\sqrt{d}} & -\frac{p}{q\sqrt{d}} \end{bmatrix}$$

for some $(p, r, q) \in S(d)$ with $q \mid j$.

- (2) $k = 3j^2 d$ for some $j \in \mathbb{Z}_{>0}$, $d \in D$, and

$$A = \begin{bmatrix} \frac{r\sqrt{3}}{q\sqrt{d}} & -\frac{p}{q\sqrt{d}} \\ \frac{p}{q\sqrt{d}} & \frac{r\sqrt{3}}{q\sqrt{d}} \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} \frac{r\sqrt{3}}{q\sqrt{d}} & \frac{p}{q\sqrt{d}} \\ \frac{p}{q\sqrt{d}} & -\frac{r\sqrt{3}}{q\sqrt{d}} \end{bmatrix}$$

for some $(p, r, q) \in S(d)$ with $q \mid j$.

Proof. Suppose $\Gamma \in C_h(\theta)$, so $\Gamma = \sqrt{k}A\Gamma_\theta$ for some $k \in \mathbb{Z}_{>0}$ and $A \in O_2(\mathbb{R})$. First notice that

$$A = \begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix} \text{ or } \begin{bmatrix} \cos t & \sin t \\ \sin t & -\cos t \end{bmatrix} \text{ for some } 0 \leq t < 2\pi.$$

Therefore, either

$$\Gamma = \frac{\sqrt{k}}{2} \begin{bmatrix} (m+n)\cos t - (m-n)\sqrt{3}\sin t & (m-2n)\cos t - m\sqrt{3}\sin t \\ (m+n)\sin t + (m-n)\sqrt{3}\cos t & (m-2n)\sin t + m\sqrt{3}\cos t \end{bmatrix} \mathbb{Z}^2,$$

or

$$\Gamma = \frac{\sqrt{k}}{2} \begin{bmatrix} (m+n)\cos t + (m-n)\sqrt{3}\sin t & (m-2n)\cos t + m\sqrt{3}\sin t \\ (m+n)\sin t - (m-n)\sqrt{3}\cos t & (m-2n)\sin t - m\sqrt{3}\cos t \end{bmatrix} \mathbb{Z}^2,$$

where m, n are as in Lemma 4.6; in any case, Γ is a sublattice of $\Lambda_h = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix} \mathbb{Z}^2$.

These observations imply the following conditions on k and t :

$$(4.8) \quad \left. \begin{aligned} \sqrt{k}((m+n)\cos t \mp (m-n)\sqrt{3}\sin t) &\in \mathbb{Z} \\ \sqrt{k}((m-2n)\cos t \mp m\sqrt{3}\sin t) &\in \mathbb{Z} \\ \sqrt{k}((m+n)\sin t \pm (m-n)\sqrt{3}\cos t) &\in \sqrt{3}\mathbb{Z} \\ \sqrt{k}((m-2n)\sin t \pm m\sqrt{3}\cos t) &\in \sqrt{3}\mathbb{Z} \end{aligned} \right\}.$$

Let us write $k = 3^u j^2 d$, where $j, d \in \mathbb{Z}_{>0}$ with d squarefree and not divisible by 3, and $u = 0, 1$. We consider two cases.

Case 1. Suppose first that $u = 0$. Then (4.8) implies that

$$(4.9) \quad \cos t = \frac{p}{q\sqrt{d}}, \quad \sin t = \frac{r}{q\sqrt{d}}\sqrt{3}$$

for some $q \mid j$.

Case 2. Suppose next that $u = 1$. Then (4.8) implies that

$$(4.10) \quad \sin t = \frac{p}{q\sqrt{d}}, \quad \cos t = \frac{r}{q\sqrt{d}}\sqrt{3}$$

for some $q \mid j$.

In both cases, the triple (p, r, q) must be a solution to the equation

$$(4.11) \quad p^2 + 3r^2 = dq^2.$$

Notice that (4.11) has integral solutions if and only if d is representable by the positive definite binary quadratic form $x^2 + 3y^2$, in which case all such solutions are given by the parameterization of Lemma 2.1 with $\alpha = 1, \beta = 0, \gamma = 3, \delta = d$. Now, it is a well known fact (see, for instance [4]) that d is representable by $x^2 + 3y^2$ if and only if its prime factorization contains only primes congruent to 1 mod 6 (which, for primes, is the same as $\equiv 1 \pmod{3}$); moreover, the number of such representations for a given d is $2^{\omega(d)+1}$, where $\omega(d)$ is the number of distinct prime divisors of d , which can be obtained as an easy consequence of unique factorization into irreducibles in the ring of Eisenstein integers. This completes the proof of the lemma. \square

An immediate corollary of this result is an explicit description of the set of all possible index values of WR sublattices of Λ_h .

Corollary 4.9. *Let \mathfrak{J} be the set of all possible values of $|\Lambda_h : \Gamma|$, where $\Gamma \in \text{WR}(\Lambda_h)$. Then*

$$(4.12) \quad \mathfrak{J} = \left\{ 3^u j^2 d(2m - n)n \quad : \quad \begin{array}{l} u = 0 \text{ or } 1, \ j, d, m, n \in \mathbb{Z}_{>0}, \\ d \text{ is 1 or a product of distinct primes} \\ \equiv 1 \pmod{3}, \gcd(m, n) = 1, 3 \nmid (m + n), 1 \leq \frac{m}{n} \leq 2 \end{array} \right\}.$$

Proof. This follows immediately by combining Lemmas 4.6 and 4.8. \square

Theorem 1.1 now follows by combining Lemmas 4.3, 4.6, and 4.7 with Corollary 4.5 (also notice references to Lemma 4.8 and Corollary 4.9 in the statement of Theorem 1.1).

5. NUMBER, MINIMA, AND INTERFERENCE OF WR SUBLATTICES OF Λ_h

In this section we investigate three related questions, which are the analogues of Questions 1, 2, and 3 of [3] for well-rounded sublattices of Λ_h . Let \mathfrak{J} be as in (4.12) and let $J \in \mathfrak{J}$.

Question 1. *Up to similarity, how many WR sublattices of Λ_h of index J are there?*

Question 2. *Which WR sublattice of Λ_h of index J has the greatest minimum?*

Question 3. *Which WR sublattice of Λ_h of index J has the highest SNR?*

In what follows, we use our parameterization in Theorem 1.1 to develop algorithmic procedures and obtain experimental data for Questions 1, 2, 3. We will write $\Gamma_\theta(m, n)$ for the lattice as in (4.6) with the specified choices of m and n ; we also define

$$(5.1) \quad A_1(p, r, q, d) = \begin{bmatrix} \frac{p}{q\sqrt{d}} & -\frac{r\sqrt{3}}{q\sqrt{d}} \\ \frac{r\sqrt{3}}{q\sqrt{d}} & \frac{p}{q\sqrt{d}} \end{bmatrix}, \quad A_2(p, r, q, d) = \begin{bmatrix} \frac{p}{q\sqrt{d}} & \frac{r\sqrt{3}}{q\sqrt{d}} \\ \frac{r\sqrt{3}}{q\sqrt{d}} & -\frac{p}{q\sqrt{d}} \end{bmatrix},$$

and

$$(5.2) \quad B_1(p, r, q, d) = \begin{bmatrix} \frac{r\sqrt{3}}{q\sqrt{d}} & -\frac{p}{q\sqrt{d}} \\ \frac{p}{q\sqrt{d}} & \frac{r\sqrt{3}}{q\sqrt{d}} \end{bmatrix}, \quad B_2(p, r, q, d) = \begin{bmatrix} \frac{r\sqrt{3}}{q\sqrt{d}} & \frac{p}{q\sqrt{d}} \\ \frac{p}{q\sqrt{d}} & -\frac{r\sqrt{3}}{q\sqrt{d}} \end{bmatrix}.$$

Considering Question 1: Let $\mathcal{N}(J)$ be the number of WR sublattices of Λ_h of index J . Then $\mathcal{N}(J)$ is equal to the number of distinct representations of J in the form

$$(5.3) \quad \begin{aligned} J &= 3^u j^2 d(2m - n)n, \text{ where } u = 0 \text{ or } 1, \ j, d, m, n \in \mathbb{Z}_{>0}, \\ &\quad d \text{ is 1 or a product of distinct primes } \equiv 1 \pmod{3}, \\ &\quad \gcd(m, n) = 1, 3 \nmid (m + n), 1 \leq \frac{m}{n} \leq 2. \end{aligned}$$

For a given J it is not difficult to count all such representations. For example, if $J = 84$ we have

$$\begin{aligned} 84 &= 3^0 \times 2^2 \times 1 \times (2 \times 5 - 3) \times 3 \\ &= 3^1 \times 2^2 \times 7 \times (2 \times 1 - 1) \times 1, \end{aligned}$$

and so $\mathcal{N}(84) = 2$, where the particular sublattices of Λ_h of index 84, up to similarity, are

$$2\Gamma_\theta(5, 3), \quad 2\sqrt{21}B_1(2, 1, 1, 7)\Lambda_h,$$

corresponding to these representations of 84 respectively. As another example, consider $J = 1925$:

$$\begin{aligned} 1925 &= 3^0 \times 5^2 \times 1 \times (2 \times 9 - 7) \times 7 \\ &= 3^0 \times 1^2 \times 7 \times (2 \times 18 - 11) \times 11 \\ &= 3^0 \times 1^2 \times 35 \times (2 \times 8 - 5) \times 5 \\ &= 3^0 \times 1^2 \times 55 \times (2 \times 6 - 5) \times 5 \\ &= 3^0 \times 5^2 \times 77 \times (2 \times 1 - 1) \times 1, \end{aligned}$$

and so $\mathcal{N}(1925) = 5$. The particular sublattices of Λ_h of index 1925, up to similarity, corresponding to the first two of these representations are

$$5\Gamma_\theta(9, 7), \quad \sqrt{7}A_1(2, 1, 1, 7)\Gamma_\theta(18, 11),$$

while the other three are sublattices similar to $\Gamma_\theta(8, 5)$, $\Gamma_\theta(6, 5)$, and $5\Lambda_h$, respectively.

Considering Question 2: Let $\Gamma \in \text{WR}(\Lambda_h)$ be a lattice with $|\Lambda_h : \Gamma| = J$. Let $\theta \in C_h$ be such that $\Gamma \in C_h(\theta)$. Then, on the one hand $\det(\Gamma) = J \det(\Lambda_h) = J\sqrt{3}/2$, and on the other $\det(\Gamma) = |\Gamma| \sin \theta$ by the parallelogram rule. Let m, n be coprime positive integers with $n \leq m \leq 2n$ and $3 \nmid (m+n)$ which correspond to the angle θ under the parameterization of (1.4), then

$$\sin \theta = \frac{\sqrt{3}(2m-n)n}{2(n^2 - nm + m^2)},$$

and so

$$(5.4) \quad |\Gamma| = \frac{J(n^2 - nm + m^2)}{(2m-n)n} \in \mathbb{Z}.$$

Hence $(2m-n)n$ must be a divisor of $J(n^2 - nm + m^2)$, which implies that $(2m-n)n \mid J$ (since by Lemma 4.3 $\gcd((n^2 - nm + m^2), (2m-n)n) = 1$). Therefore our integers m, n must satisfy the following conditions:

- (1) $m, n > 0$ and $\gcd(m, n) = 1$
- (2) $1 \leq \frac{m}{n} \leq 2$
- (3) $3 \nmid (m+n)$
- (4) $(2m-n)n \mid J$
- (5) $\frac{J(n^2 - nm + m^2)}{(2m-n)n}$ is representable by the quadratic form $x^2 - xy + y^2$,

and, to maximize $|\Gamma|$, among all such m, n we want to choose a pair that maximizes the quotient $(n^2 - nm + m^2)/(2m-n)n$. We can write $m = \beta n$, where $\beta \in [1, 2]$, and define

$$f(\beta) = \frac{n^2 - nm + m^2}{(2m-n)n} = \frac{\beta^2 - \beta + 1}{2\beta - 1},$$

which is a decreasing function on the interval $[1, (1 + \sqrt{3})/2]$ and an increasing function on the interval $[(1 + \sqrt{3})/2, 2]$. In fact, $f(\beta)$ reaches its maximum at the endpoints of the interval, $\beta = 1, 2$, which are achieved by the pairs $(m, n) = (1, 1)$ and $(2, 1)$, respectively. The choice $(m, n) = (2, 1)$, however, does not satisfy the condition (3) above, while the choice $(m, n) = (1, 1)$ corresponds to the similarity

class $C_h(\pi/3) = \langle \Lambda_h \rangle$. This means that whenever J is representable by the quadratic form $x^2 - xy + y^2$, then $|\Gamma|$ reaches its maximum on $WR(\Lambda_h)$ at an ideal sublattice of index J ; this conclusion is consistent with Theorem 3 of [3]. As indicated in (12) of [3], this happens for all values of J with prime factorization of the form

$$(5.5) \quad J = 3^k \prod_{p_i \equiv 1 \pmod{3}} p_i^{l_i} \prod_{q_j \equiv -1 \pmod{3}} q_j^{2m_j},$$

where $k, l_i, m_j \in \mathbb{Z}_{\geq 0}$. On the other hand, there exist WR sublattices of Λ_h of index J for many values of J not in the form (5.5); in these situations, verifying conditions (1)-(5) above for every divisor of J presents a finite search algorithm for the similarity class containing a WR sublattice Γ of Λ_h of index J with maximal $|\Gamma|$. The next lemma allows to eliminate some of the values of the index J for which WR sublattices of Λ_h do not exist.

Lemma 5.1. *Suppose that $J \in \mathbb{Z}_{>0}$ is not of the form (5.5), and satisfies one of the following:*

- (1) J is a prime
- (2) $J = pq$, where p, q are odd primes with $q > 3p$
- (3) $J = 2p$, where p is an odd prime

Then Λ_h does not have a WR sublattice of index J .

Proof. Suppose there exists $\Gamma \in WR(\Lambda_h)$ with $|\Lambda_h : \Gamma| = J$, where J is not of the form (5.5). Then $\Gamma \in \langle \Gamma_\theta \rangle$ for some $\Gamma_\theta \sim \Lambda_h$ as in Theorem 1.1, meaning that

$$J = k(2m - n)n$$

for some $m, n, k \in \mathbb{Z}_{>0}$ with $\gcd(m, n) = 1$, $n \leq m \leq 2n$, $3 \nmid (m + n)$, and $m, n \neq 1$.

First suppose that J is a prime, then $k = 1$, $n = J$, and $m = \frac{J+1}{2}$ (since $n \neq 1$). In this case, however, $\frac{J+1}{2} < J$, contradicting the condition $n \leq m$; hence this is impossible.

Next assume that $J = pq$, where p, q are odd primes with $q > 3p$. If $k = p$ or q , then $(2m - n)n$ is a prime, and so we are back in the situation above. Then $k = 1$, $n = p$, and $2m - p = q$, meaning that $m = (p + q)/2 > 2p = 2n$, which contradicts the condition $m \leq 2n$; hence this is impossible.

Finally, suppose that $J = 2p$, where p is an odd prime. If $k = 2$ or p , then $(2m - n)n$ is a prime, and so we are back in the situation above. Then $k = 1$, $n = 2$, and $2m - 2 = p$, which is not possible since p is odd. \square

Using Lemma 5.1, we can immediately eliminate many of the small values of the index, such as $J = 2, 5, 6, 10, 11, 14, 17, 22, 23, 26, 29, 33, 34, 38, 41, 46, 47, 53, 59$, etc. In the table below, we exhibit a few examples we computed for some small values of J not in the form (5.5), for which WR sublattices of Λ_h of index J exist.

In fact, there exists an easy test to check our work: if $\Gamma \in WR(\Lambda_h)$ with $|\Lambda_h : \Gamma| = J$ and $|\Gamma| = M$, then $\Gamma \in C_h(\theta)$ with

$$(5.6) \quad \cos \theta = \frac{\sqrt{4M^2 - 3J^2}}{2M} \in \mathbb{Q}.$$

It is now easy to verify that for any value M of $|\Gamma|$ larger than those in the table above, the expression in (5.6) would not be rational.

Considering Question 3: As above, suppose that $\Gamma \in C_h(\theta)$ for some $\theta \in C_h$ is a lattice with $|\Lambda_h : \Gamma| = J$ where J is fixed. Recall that the total interference of Γ is given by $E_\Gamma(2)$, where $E_\Gamma(s)$ is as in (1.8), and $\text{SNR}(\Gamma)$ is defined in (1.9). Here we show that Question 3 can be reduced to Question 2. Notice that this is not generally so for *any* (not necessarily WR) sublattices of Λ_h , as indicated in [3].

Lemma 5.2. *A WR sublattice $\Gamma \subseteq \Lambda_h$ maximizes $\text{SNR}(\Gamma)$ among all WR sublattices of Λ_h of index J if and only if it maximizes $|\Gamma|$.*

Proof. Let $M = |\Gamma|$, and let $Q_\Gamma(x, y)$ be the quadratic form of Γ corresponding to a minimal basis, then

$$Q_\Gamma(x, y) = M(x^2 + y^2 + 2xy \cos \theta).$$

The Epstein zeta-function of Γ is then given by

$$E_\Gamma(s) = \sum_{x, y \in \mathbb{Z} \setminus \{0\}} Q_\Gamma(x, y)^{-s} = \frac{1}{M^s} g_\Gamma(\theta),$$

where $g_\Gamma(\theta) = \sum_{x, y \in \mathbb{Z} \setminus \{0\}} \frac{1}{(x^2 + y^2 + 2xy \cos \theta)^s}$. Then

$$\begin{aligned} \frac{d}{d(\cos \theta)} g_\Gamma(\theta) &= \sum_{x, y \in \mathbb{Z} \setminus \{0\}} \frac{2sxy}{(x^2 + y^2 + 2xy \cos \theta)^{s+1}} \\ &= \sum_{x, y \in \mathbb{Z}_{>0}} \left(\frac{4sxy}{(x^2 + y^2 + 2xy \cos \theta)^{s+1}} - \frac{4sxy}{(x^2 + y^2 - 2xy \cos \theta)^{s+1}} \right) \\ &< 0, \end{aligned}$$

meaning that $g_\Gamma(\theta)$ is a decreasing function of $\cos \theta$ for $\theta \in [\pi/3, \pi/2]$. Now $\cos \theta$ is given by (5.6), and is easily seen to be an increasing function of M . Therefore for all real values of $s > 1$, $E_\Gamma(s)$ is a decreasing function of M , in particular meaning that the total interference of Γ is minimized (and hence $\text{SNR}(\Gamma)$ is maximized) if and only if $|\Gamma|$ is maximized. \square

Lemma 5.2 now implies that in order to find a WR sublattice of Λ_h of fixed index that maximizes SNR, we can follow the algorithmic procedure described in our consideration of Question 2 above.

TABLE 1. Examples of $\Gamma \in \text{WR}(\Lambda_h)$ of fixed index J maximizing $|\Gamma|$.

$J = \Lambda_h : \Gamma $	Maximal $ \Gamma $	Lattice Γ
8	7	$\Gamma_\theta(3, 2)$
15	13	$\Gamma_\theta(4, 3)$
21	19	$\Gamma_\theta(5, 3)$
24	21	$\sqrt{3}B_1(1, 1, 2, 1)\Gamma_\theta(3, 2)$
32	28	$2\Gamma_\theta(3, 2)$
35	31	$\Gamma_\theta(6, 5)$
40	37	$\Gamma_\theta(7, 4)$
45	39	$\sqrt{3}B_1(1, 1, 2, 1)\Gamma_\theta(4, 3)$
55	49	$\Gamma_\theta(8, 5)$
60	52	$2\Gamma_\theta(4, 3)$
65	61	$\Gamma_\theta(9, 5)$

6. COMBINATORIAL STRUCTURE IN THE EISENSTEIN TRIPLES

As a part of the parameterization of similarity classes of WR sublattices of \mathbb{Z}^2 in [8], it has been shown that the set of these similarity classes has the structure of a non-commutative monoid generated by an infinite family of matrices from $\text{GL}_3(\mathbb{Z})$. The corresponding matrices can be characterized as words of a certain shape in three particular matrices that can be used to generate all primitive Pythagorean triples from $(3, 4, 5)$ by left multiplication. The existence of these generating matrices for primitive Pythagorean triples has long been known (see [8] for details). In this section we will investigate a similar generating family of matrices for primitive Eisenstein triples, and use them to explore the combinatorial structure of the set of similarity classes of WR sublattices of Λ_h .

Let P_E be the set of all primitive Eisenstein triples as defined in section 4 above. Let also $G_E = \langle U, M_1, M_2, M_3 \rangle$ be the non-commutative monoid generated by the 3×3 matrices $U, M_1, M_2, M_3 \in \text{GL}_3(\mathbb{Z})$, defined as follows:

$$U = \begin{bmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad M_1 = \begin{bmatrix} 3 & -4 & 4 \\ 7 & -7 & 8 \\ 6 & -6 & 7 \end{bmatrix}, \quad M_2 = \begin{bmatrix} -4 & 3 & 4 \\ -7 & 7 & 8 \\ -6 & 6 & 7 \end{bmatrix}, \quad M_3 = \begin{bmatrix} 1 & 3 & 4 \\ 0 & 7 & 8 \\ 0 & 6 & 7 \end{bmatrix}.$$

Lemma 6.1. G_E acts on the set P_E by left multiplication:

$$(6.1) \quad M(a, b, c) = M \begin{bmatrix} a \\ b \\ c \end{bmatrix},$$

for every $M \in G_E$ and $(a, b, c) \in P_E$.

Proof. A direct verification (for instance, using Maple or SAGE mathematical software packages) shows that for every $1 \leq i \leq 3$ and $(a, b, c) \in P_E$, $M_i(a, b, c) \in P_E$; also $U(a, b, c) = (b - a, b, c) \in P_E$. Since G_E is generated by U, M_1, M_2, M_3 , it follows that for every $M \in G_E$ and $(a, b, c) \in P_E$, we have $M(a, b, c) \in P_E$. \square

Remark 6.1. Computational evidence (using SAGE) suggests that perhaps all primitive Eisenstein triples can be obtained in this way, starting from $(0, 1, 1)$; in other words, it seems likely that for each $(a, b, c) \in P_E$ there exists $M \in G_E$ such that $M(0, 1, 1) = (a, b, c)$. One matrix from the monoid G_E has previously been found in [2].

The action of Lemma 6.1 induces an action on the set of similarity classes of WR sublattices of Λ_h . The similarity classes however are parameterized not by the set P_E of primitive Eisenstein triples (a, b, c) , but by the set of associated pairs of these triples $\langle a, b, c \rangle$ as defined in section 4 (see Lemma 4.3 and definition right before it); let us write \mathfrak{P}_E for this set. Recall that the elements of an associated pair are related by $(b - a, b, c) = U(a, b, c)$. Hence we can think of the set \mathfrak{P}_E as the set P_E modulo the equivalence relationship: $(a', b', c') \sim (a, b, c)$ when $(a', b', c') = U(a, b, c)$. For each associated pair in \mathfrak{P}_E , let us call the triple with $b > 2a$ the *upper* triple, denoted $(a, b, c)_u$, and the one with $b < 2a$ the *lower* triple, denoted $(a, b, c)_l$. Now let us write $M_4 = M_1U, M_5 = M_2U$ and define a sub-semigroup of G_E , $G'_E = \langle M_1, M_2, M_3, M_4, M_5 \rangle$. For each $M \in G'_E$, $\langle a, b, c \rangle \in \mathfrak{P}_E$ define

$$(6.2) \quad M \langle a, b, c \rangle = \langle M(a, b, c)_u \rangle,$$

where $M(a, b, c)_u$ is as in (6.1) for the vector corresponding to the upper triple of $\langle a, b, c \rangle$, and so $M \langle a, b, c \rangle$ is the associated pair of the triple corresponding to the vector $M(a, b, c)_u$ in \mathfrak{P}_E .

Lemma 6.2. G'_E acts on \mathfrak{P}_E by $M \langle a, b, c \rangle$ for every $M \in G'_E$, $\langle a, b, c \rangle \in \mathfrak{P}_E$.

Proof. This follows immediately by combining Lemma 6.1 with definition (6.2). \square

Computational evidence (using SAGE) suggests that there are no relations between the generators M_1, \dots, M_5 of G'_E , and that every element of \mathfrak{P}_E can be obtained from $\langle 0, 1, 1 \rangle$ by the action of some $M \in G'_E$. In fact, let γ_1, γ_2 be the larger and the smaller roots of the polynomial $143t^2 - 252t + 111$, respectively, and for each $(a, b, c)_u \in P_E$ with $a > 0$ define

$$(x, y, z) = \begin{cases} M_1^{-1}(a, b, c)_u & \text{if } \gamma_1 < c/b \\ M_4^{-1}(a, b, c)_u & \text{if } 7/8 \leq c/b < \gamma_1 \\ M_5^{-1}(a, b, c)_u & \text{if } \gamma_2 < c/b < 7/8 \\ M_2^{-1}(a, b, c)_u & \text{if } 13/15 \leq c/b < \gamma_2 \\ M_3^{-1}(a, b, c)_u & \text{if } c/b < 13/15. \end{cases}$$

In each of these cases, computational evidence (using SAGE) suggests that (x, y, z) is a primitive upper Eisenstein triple with $z < c$, meaning that \mathfrak{P}_E is the orbit of $\langle 0, 1, 1 \rangle$ under the action of G'_E (and so P_E is the orbit of $(0, 1, 1)$ under the action of G_E). These observations conjecturally imply a nice combinatorial structure on the set \mathfrak{P}_E (and hence on the set of similarity classes of WR sublattices of Λ_h) of two quinary trees joint at the roots, as illustrated in Figure 3.

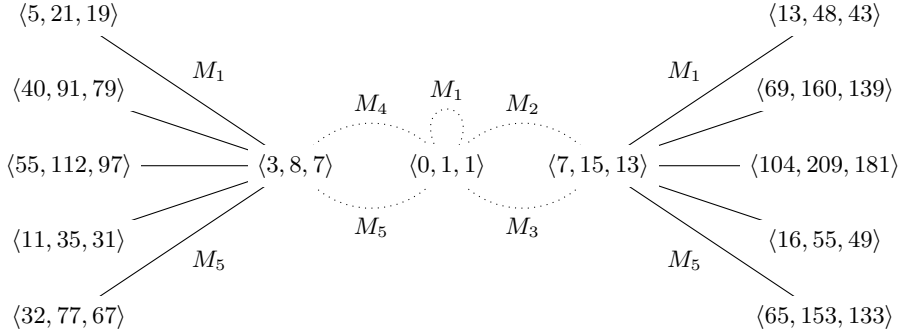


FIGURE 3. Structure of the set \mathfrak{P}_E induced by the action of the monoid G'_E

Acknowledgment. We would like to thank the NSF supported Claremont Colleges REU program, under the auspices of which this work was done during the Summer of 2009. We also want to thank Chris Towse for his helpful comments on the subject of this paper.

REFERENCES

- [1] A. H. Banihashemi and A. K. Khandani. On the complexity of decoding lattices using the Korkin-Zolotarev reduced basis. *IEEE Trans. Inform. Theory*, 44(1):162–171, 1998.
- [2] F. Barnes. Pythagorean triples, etc. <http://pythag.net/triples.html>.
- [3] M. Bernstein, N. J. A. Sloane, and P. E. Wright. On sublattices of the hexagonal lattice. *Discrete Math.*, 170(1-3):29–39, 1997.
- [4] J. C. Butcher. Mathematical Miniature 9: Hardy’s taxi, $x^2 + 3y^2 = p$ and Michael Lennon. *New Zealand Math. Soc. Newslett.*, 76:18–19, 1999.
- [5] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices, and Groups*. Springer-Verlag, Third edition, 1999.
- [6] L. Fukshansky. Revisiting the hexagonal lattice: on optimal lattice circle packing. *to appear in Elem. Math.*
- [7] L. Fukshansky. On distribution of well-rounded sublattices of \mathbb{Z}^2 . *J. Number Theory*, 128(8):2359–2393, 2008.
- [8] L. Fukshansky. On similarity classes of well-rounded sublattices of \mathbb{Z}^2 . *J. Number Theory*, 129(10):2530–2556, 2009.
- [9] L. Fukshansky and S. Robins. Frobenius problem and the covering radius of a lattice. *Discrete Comput. Geom.*, 37(3):471–483, 2007.
- [10] J. Martinet. *Perfect Lattices in Euclidean Spaces*. Springer-Verlag, 2003.
- [11] C. McMullen. Minkowski’s conjecture, well-rounded lattices and topological dimension. *J. Amer. Math. Soc.*, 18(3):711–734, 2005.

DEPARTMENT OF MATHEMATICS, 850 COLUMBIA AVENUE, CLAREMONT MCKENNA COLLEGE,
CLAREMONT, CA 91711

E-mail address: `lenny@cmc.edu`

DEPARTMENT OF MATHEMATICS, LOYOLA MARYMOUNT UNIVERSITY, 1 LMU DRIVE, LOS AN-
GELES, CA 90045

E-mail address: `daniel.ross.moore@gmail.com`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WASHINGTON, Box 354350, SEATTLE, WA
98195-4350

E-mail address: `andrew.ohana@gmail.com`

DEPARTMENT OF MATHEMATICS, SAN FRANCISCO STATE UNIVERSITY, 1600 HOLLOWAY AVENUE,
SAN FRANCISCO, CA 94132

E-mail address: `whitneyzeldow@hotmail.com`